REMARKS

Claims 3, 5-29, 32, 34-59, 61, and 62 are pending, in which claims 1, 2, 4, 30, 31, 33, and 60 were previously canceled. No claim is canceled, withdrawn, currently amended, or newly added.

The Office Action mailed May 5, 2004 rejected claims 3, 5-7, 10-21, 25, 26, 29, and 32 under 35 U.S.C. § 102 as anticipated by *Alles et al.* (US 6,499,976), claims 8, 22, 24, 27, and 28 as obvious under 35 U.S.C. § 103 based on *Alles et al.* in view of *Dillon et al.* (US 6,519,651), claims 61 and 62 as obvious under 35 U.S.C. § 103 based on *Alles et al.* in view of *Dillon et al.* in view of *Milton et al.* (US 6,721,333), claim 23 as obvious under 35 U.S.C. § 103 based on *Alles et al.* in view of *Dillon et al.* in view of *Jorgensen* (US 6,590,885), and claim 9 as obvious under 35 U.S.C. § 103 based on *Alles et al.* in view of *Klaus* (US 5,892,903).

Independent claim 3 recites "a spoofing element which only **spoofs** connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired." Independent claim 32 recites "**spoofing** only connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired."

For a supposed teaching of these features, the Office Action, on page 3, applies *Alles et al.*, citing col. 12: 39-67, and col. 9: 44 – col. 10: 11. The Office Action also refers to col. 12: 52-58 within the already cited passage of col. 12: 39-67. Neither these passages, nor any other passages within *Alles et al.*, disclose any manner of "spoofing," much less "spoofing only connections of the first type associated with at least one of applications with high throughput and applications for which reduced startup latency is desired." Applicants do not understand why this claim language continues to be ignored.

Alles et al. provides on col. 9: 44 – col. 10: 11 the following:

> FIG. 3 is a block diagram illustrating the details of ISN 150 in one embodiment. ISN 150 may include access ports (310-A and 310-B), trunk ports (320-A, 320-B and 320-C), switch fabric 340, packet service cards 350-A and 350-B, and route management card 360. Trunk ports 320-A, 320-B and 320-C will be collectively or individually referred to by 320 as will be clear from the context. Similar convention is used with reference to other components described in the present application.
>
> It may be noted that packet service cards 350 are physically separated from ports 310 and 320. The physical separation enables the number of packet service cards 350 to be changed independent of the number of ports 310 and

320, and vice versa. Such a flexibility enables the ISN 150 to scale well to serve a large number of subscribers.
Access ports 310 provide the necessary physical interface to receive and send bit groups in a pre-specified format. Protocols such as Sonet may be used for high speed interface. For purposes of illustration, access ports 310 will be assumed to send and receive data in the form of ATM cells. Each subscriber port 310 forwards the ATM cells to switch fabric 340.

Trunk ports 320 provide high speed access lines for internet access to subscribers. Trunk ports 320 receive ATM cells (or other bit groups) from switch fabric 340, and forwards the cells on the corresponding lines as specified by the channel identifier (or other destination address). Similarly, trunk ports 320 may receive data bit groups in the form of ATM cells or IP packets from the Internet and send the data bit groups to switch fabric 340. In this reception scenario, higher level protocol information (e.g., IP header) may need to be examined to determine the subscriber associated with the received data bits. The determination may form the basis for allocation of the data bits to a specific processor group for further processing.

The above passage merely discloses the roles of the trunk ports 320 in the Internet Service Node (ISN) 150, and is completely silent on "spoofing" any connection.

The other cited passage of col. 12: 39-67 states the following:

At least some of the service rule parameters are readily available up-front and can thus be statically translated into corresponding processing rule parameters. Thus, assuming the IP addresses SubsA and Office1 of service rule 510 are known beforehand, two processing rules may be generated from the service rule as the TCP port number for IMAP is pre-specified.

However, if one of the IP addresses (e.g., SubsA) is to be generated dynamically, for example as the user system needs to establish a dial-in connection, user interface 470 may dynamically generate the processing rules after the user is assigned an IP address. The processing rule may also be instantiated dynamically.

Service rule 520 attempts to accept and encrypt all HTTP, SMTP, and TELNET traffic from and to SubsA. Processing rule(s) may be generated for each of HTTP, SMTP, and TELNET. The protocol types and port numbers for these three applications are pre-specified, and accordingly processing rules may be generated statically assuming the IP addresses (for SubsA and other offices) are also known.

Service rule 530 accepts all HTTP traffic to SubsA-Web-Srvr. Service rule 540 accepts all smtp traffic with SubsA-Mail-Srvr. Service rule 550 accepts all traffic from SubsA-Subsets. Service rule 560 drops (discards) all other data and makes a log of the dropped data for later accounting and analysis. As may be readily appreciated, the approach of FIG. 5A can be used to implement security requirements specific to a subscriber. Different subscribers may have different policy rules to suit their individual needs.

This cited passage, despite its length, is also lacking in any discussion of "spoofing." In fact, Applicants' study of the reference reveals only a mention of "anti-spoofing" in the context of security in col. 7: 52-60. This is consistent with the Examiner's recognition that Alles et al. fails to disclose "a spoofing element which spoofs acknowledgements" (on page 7, with respect to the rejection of claim 8), as well as the acknowledgement that Alles et al. fails to disclose "a spoofing element which spoofs a three way handshake" (on page 9, with respect to the rejection of claim 9).

In addition, Applicants maintains that there is no disclosure of spoofing "only connections ... associated with at least one of applications with high throughput and applications for which reduced startup latency is desired." The Office Action explains (on pages 3 and 11) that because Alles et al. discloses that "the processing rule processes packets received from a designated IP address 'SubsA' connected through one of the ports and discards all other packet" that this is a disclosure of "only spoofs connections of the first type associated with at least one of applications." At best, Alles et al. discloses that traffic from SubsA-Subsets are accepted, and other traffic is not. Alles et al. does not disclose that the applications are "associated with at least one of applications with high throughput and applications for which reduced startup latency is desired." Alles et al. merely states that HTTP traffic can be accepted from and to SubsA (col. 12: 52-59). The Office Action makes the technical leap that HTTP traffic is "associated with at least one of applications with high throughput and applications for which reduced startup latency is desired" without any factual grounding in Alles et al.

As anticipation under 35 U.S.C. § 102 requires that each and every element of the claim be disclosed in a prior art reference, based on the foregoing, it is clear that Alles et al. does not anticipate claims 3 and 32, particularly with respect to the feature of "spoofing."

Thus, Applicants respectfully request the withdrawal of the rejection under § 102, and the indication that independent claims 3 and 32 are allowable, along with dependent claims 5-7, 10-21, 25, 26, and 29. These dependent claims are further patentable on their own merits. For example, claim 5 recites "wherein said spoofing element assigns spoofing resources, including buffer space and control blocks, to the spoofed connections." The Office Action, on page 8, recites this claim by citing col. 8: 4-10, which discloses the following:

> Conditions may be specific to the type of service policy being implemented. For example, **a subscriber may be permitted higher bandwidth during non-business hours**. Another subscriber may have the data being given a lower priority if the data is destined to a specific subscriber during a specified time of

day. Examples of the conditions are described in further detail below with reference to FIG. 5B.

As proffered above, Alles et al. provides no capability to spoof, and thus, cannot assign resources towards that capability. Moreover, the above passage simply states in general terms that higher bandwidth can be permitted based on a schedule. In contrast, the claim language specifically recites assignment of "resources, including buffer space and control blocks."

As another example, dependent claim 15 recites "wherein said path selection element can select up to N paths (N>1), where the Nth path is selected only if the (N-1)th path fails." The Office Action refers to col. 6: 1-34 of Alles et al. for such a disclosure. Applicants fail to see the relevance of this cited passage, which discloses that "Multiple TCP connections may be used to implement an application" (col. 6: 10-11) without any mention of failed paths or selection of paths, much less in the manner claimed.

As for claim 17, which recites "wherein said path selection element defines the at least one path selection rule in a path selection profile," the Office Action refers to the same irrelevant passage, col. 6: 1-34. As noted, because Alles et al. provides no disclosure of failed paths or any selection of paths, there can be no disclosure of the claimed "path selection profile."

Dependent claim 18 recites "a compression/encryption element, which compresses and/or encrypts data associated with connections of the first type for transmission across connections of the second type." The Office Action refers to col. 12: 24-38, which in pertinent part, provides a general discussion on encrypting "matching data using 3xDES encryption protocol," without any mention of "compression."

As seen from the above analysis of the dependent claims, the Office Action repeatedly has offered citations to irrelevant passages as rationale for the rejections. 35 U.S.C. § 132 requires the Director to "notify the applicant thereof, stating the reasons for such rejection." This section is violated if the rejection "is so uninformative that it prevents the applicant from recognizing and seeking to counter the grounds for rejection." Chester v. Miller, 15 USPQ2d 1333 (Fed. Cir. 1990). This policy is captured in the Manual of Patent Examining Procedure. For example, MPEP § 706 states that "[t]he goal of examination is to clearly articulate any rejection early in the prosecution process so that applicant has the opportunity to provide evidence of patentability and otherwise respond completely at the earliest opportunity." Furthermore, MPEP § 706.02(j) indicates that: "[i]t is important for an examiner to properly communicate the basis for a rejection so that the issues can be identified early and the

applicant can be given fair opportunity to respond." Unfortunately, the Examiner 's only discussion of the claim features involve citing to seemingly irrelevant passages.

Turning now to the obviousness rejection of claims 8, 22, 24, 27, and 28 over Alles et al. in view of Dillon. In support of this rejection, the Office Action draws the conclusion that the proposed modification of the Alles et al. system is obvious because "doing so would allow the faster communication over the network apparatus by discarding packets with spoofed acknowledgements and therefore allocating more network resources for processing of other data packets received by the network." In drawing this conclusion, the Office Action has ignored the basic tenets of obviousness. In rejecting claim under 35 U.S.C. § 103, the Examiner must provide a factual basis to support the obviousness conclusion. In re Warner, 379 F.2d 1011, 154 USPQ 173 (CCPA 1967); In re Lunsford, 357 F.2d 385, 148 USPQ 721 (CCPA 1966); In re Freed, 425 F. 2d 785, 165 USPQ 570 (CCPA 1970). Based upon the objective evidence of record, the Examiner is required to make the factual inquiries mandated by Graham v. John Deere Co., 86 S. Ct. 684, 383 U.S. 1, 148 USPQ 459 (1966). The Examiner is also required to explain how and why one having ordinary skill in the art would have been led to modify an applied reference to arrive at the claimed invention. Uniroyal, Inc. v. Rudkin-Wiley Corp., 837 F.2d 1044, 5 USPQ2d 1434 (Fed. Cir. 1988). As explained with respect to the allowability of independent 3, the Alles et al. system operates without any spoofing capability -- which is understandable as "a spoofing protocol compensates for the long propagation delays inherent to satellite communication" (Abstract of Dillon). The terrestrial system of Alles et al. is not concerned with such delays, and thus, would not aim to introduce unnecessary complexity.

As for the obviousness rejection of claims 61 and 62 over the several combinations of Alles et al., Dillon et al., and Milton et al., the combination of Alles et al. and Dillon et al. is improper, as explained earlier. The addition of Milton et al. does not correct this impropriety.

Similarly, the obviousness rejection of claim 23 over the combination of Alles et al., Dillon et al., and Jorgensen. is unsustainable, in that combination of Alles et al. and Dillon et al. is improper, lacking in factual and legal bases.

Regarding the rejection of claim 9, the Office Action proposes the combination of Alles et al. and Klaus, whereby the Office Action applies Klaus for a supposed teaching of "a spoofing element which spoofs a three way handshake." Klaus discloses an IP spoofing attack generator 32 (FIG. 2), in a security context. By contrast, the claim language of "spoof" has context in the networking sense; see e.g., Specification, page 4, lines 7-11, and page 13, lines

15-31. Further, Newton's Telecom Dictionary (16th Edition) defines spoofing as follows: "3. A networking term. Spoofing is a method by which a receiving device is spoofed, or fooled, into thinking that data are being transmitted in order that the device doesn't 'time out' the data session." Thus, even if Klaus can be properly combined with Alles et al., the claimed spoofing element is not taught.

Furthermore, it is not understood how the Examiner intends to employ this IP spoofing attack generator in the Alles et al. system. This is simply hindsight. It is well settled that it is impermissible simply to engage in hindsight reconstruction of the claimed invention, using Applicant's structure as a template and selecting elements from the references to fill in the gaps. In re Gorman, 933 F.2d 982, 18 USPQ2d 1885 (Fed. Cir. 1991). Recognizing, after the fact, that a modification of the prior art would provide an improvement or advantage, without suggestion thereof by the prior art, rather than dictating a conclusion of obviousness, is an indication of improper application of hindsight considerations. Simplicity and hindsight are not proper criteria for resolving obviousness. In re Warner, 397 F.2d 1011, 154 USPQ 173 (CCPA 1967).

In view of the foregoing, Applicants urge the indication that 8, 9, 22-24, 27, and 28 are in condition for allowance.

Favorable consideration of this application is respectfully requested. If any unresolved issues remain, it is respectfully requested that the Examiner telephone the undersigned attorney at (301) 601-7252 so that such issues may be resolved as expeditiously as possible. All correspondence should continue to be directed to our below-listed address.

Respectfully submitted,

29 June, 2004

Craig L. Plastrik
Attorney for Applicant
Registration No. 41,254

THE DIRECTV GROUP, INC.
(formerly Hughes Electronics Corporation)
Customer No. 20991